The Variant of Remote Set Problem on Lattices

Wenwen Wang[1,2,3(✉)], Kewei Lv[1,2(✉)], and Jianing Liu[1,2,3]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences,
Beijing 100093, China
{wangwenwen,lvkewei,jianingliu}@iie.ac.cn
[2] Data Assurance Communication Security Research Center,
Chinese Academy of Sciences, Beijing 100093, China
[3] University of Chinese Academy Sciences, Beijing 100049, China

Abstract. In 2015, Haviv proposed the Remote Set Problem (RSP) on lattices and gave a deterministic algorithm to find a set containing a point which is $O(\sqrt{k/n})$ far from the lattice in ℓ_p norm for $2 \leq p \leq \infty$, where n is the lattice rank and k divides n. Inspired by it, we propose the variant of Remote Set Problem on Lattices (denoted by V-RSP) that only depends on parameter $\gamma \leq 1$. We obtain that the complexity classes that V-RSP belong to with the change of parameter γ. Using some elementary tools, we can solve V-RSP that can find a set containing a point which is $O(k/n)$ far from the lattice in any ℓ_p norm for $1 \leq p \leq \infty$. Furthermore, we also study relationships between ℓ_2 distance from a point to a lattice $\boldsymbol{\mathcal{L}}$ and covering radius $(\rho^{(p)}(\boldsymbol{\mathcal{L}}))$, where $\rho^{(p)}(\boldsymbol{\mathcal{L}})$ is defined with respect to the ℓ_p norm for $1 \leq p \leq \infty$, here, for $p = \infty$, our proof does not rely on Komlós Conjecture.

Keywords: Lattice · Equivalent norms · The variant of remote set problem · Hölder's inequality

1 Introduction

A lattice is a discrete additive subgroup of $\mathbb{R}^m$ and is the set of all integer linearly combinations of n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ in $\mathbb{R}^m$, where n is the rank of the lattice, m is the dimension of the lattice and $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is called a lattice basis. Gauss [7] gave an algorithm to find the shortest vector in any two dimension lattice that originated the study of lattices. Since then, many different lattice problems were proposed. In 1996, Ajtai [2] showed that finding relatively short nonzero vectors is as hard as approximating shortest vector problems in the worst case in a family of random lattice. These random lattices can be used for cryptography. Hence, the study of lattices gains a lot of attention from a computational point of view.

There are two classical problems in lattices. The first is the Shortest Vector Problem (SVP): given a lattice, find the shortest non-zero lattice vector. The second is the Closest Vector Problem (CVP): given a lattice and a target vector, find the closest lattice vector to the target vector.

K.-Y. Lam et al. (Eds.): ICICS 2016, LNCS 9977, pp. 124–133, 2016.
DOI: 10.1007/978-3-319-50011-9_10

The covering radius $\rho^{(p)}(\boldsymbol{\mathcal{L}})$ of lattice $\boldsymbol{\mathcal{L}}$ is the maximum ℓ_p distance of a point in the linear span of $\boldsymbol{\mathcal{L}}$ from the lattice, where $\rho^{(p)}(\boldsymbol{\mathcal{L}})$ is measured with respect to the ℓ_p norm for $1 \leq p \leq \infty$. The covering radius problem is to find $\rho^{(p)}(\boldsymbol{\mathcal{L}})$ for a given lattice $\boldsymbol{\mathcal{L}}$. The Covering Radius Problem (CRP) is also an important lattice problem and the exact CRP is in Π_2 at the second level of the polynomial hierarchy. Computing the covering radius of a lattice is a classic problem in geometry of numbers, but it has received so far little attention from an algorithmic point of view. In 2004, Micciancio [16] showed that finding collision of some hash function can be reduced to approximate CRP of lattices, where CRP only is used to connect the average and worst case complexity of lattice problems. Motivated by [8], Guruswami et al. [10] initiated the study of computation complexity for CRP, and showed that CRP_2 lies in AM, $\mathrm{CRP}_{\sqrt{n/\log n}}$ lies in coAM and $\mathrm{CRP}_{\sqrt{n}}$ lies in $NP \cap coNP$ which implies that under Karp reductions $\mathrm{CRP}_{\sqrt{n}}$ is not NP-hard unless $NP = coNP$. But they did not give some hardness results for CRP [10]. Peikert [18] showed that $\mathrm{CRP}_{\sqrt{n}}$ lies in coNP in the ℓ_p norm for $2 \leq p \leq \infty$. The first hardness result for CRP was presented by Haviv and Regev, they proved that there exists some constant such that it is Π_2-hard in the ℓ_p norm for any sufficiently large value of p [12]. In 2015, Haviv [13] proposed the Remote Set Problem (RSP) on lattices which can be viewed as a generalized search variant of CRP. The goal of RSP is to find a set of points containing a point which is far from the lattice under a deterministic algorithm in ℓ_p norm for $2 \leq p \leq \infty$. By the deterministic polynomial time algorithm for RSP, Haviv showed that $\mathrm{CRP}_{\sqrt{n/\log n}}$ lies in NP which improved the factor from [10], and proved that approximation GAPCRP can be reduced to approximation GAPCVP.

In the study of CRP, we usually find a point whose distance from the lattice approximates the covering radius. There is a deterministic construction of all the M^n linear combinations of the n basis vectors with all coefficients in $\{0, 1/M, \ldots, 1-1/M\}$ where M is an integer. Micciancio [10] showed that there exists at least one of them whose distance from the lattice approximates the covering radius to within a factor of $1 - 1/M$. In order to decrease the number of exponential points in the above construction [10], Haviv proposed RSP and gave a deterministic algorithm (see Sect. 3) that outputs $n/k \cdot 2^k$ linear combinations of vectors in basis with coefficient in $\{0, 1/2\}$ (i.e. $M = 2$) by partitioning the n basis vectors into n/k sets of size k [13]. The algorithm outputs a set of $n/k \cdot 2^k$ points containing a point whose ℓ_p distance from a lattice is at least $1/(2c_p) \cdot \sqrt{k/n} \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ for $2 \leq p < \infty$, where c_p is a constant. For $p = \infty$, there is a similar result. Haviv analyzed RSP with respect to Banach spaces and obtained the results which hold for any ℓ_p norm for $2 \leq p \leq \infty$. Here, we will consider the variant of Remote Set Problem which is denoted by V-RSP with respect to any ℓ_p norm for $1 \leq p \leq \infty$.

Our Contributions. In this paper, we consider the variant of Remote Set Problem (V-RSP) on lattices. Using elementary method, we prove that V-RSP can be adapted to any ℓ_p norm for $1 \leq p \leq \infty$.

The Remote Set Problem [13] is defined and depends on two parameters d, γ to be minimized, where d is the size of the output set $\boldsymbol{S}$ by the algorithm for RSP and $\gamma \geq 1$ is the remoteness parameter for which $\boldsymbol{S}$ contains a point whose distance from $\boldsymbol{\mathcal{L}}$ is at least $1/\gamma \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$. Here, we give the definition for V-RSP which only depends on remoteness parameter γ:

- $\gamma \leq 1$ is a parameter such that the algorithm finds a set containing a point whose distance from $\boldsymbol{\mathcal{L}}$ is at least $\gamma \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ for the input lattice $\boldsymbol{\mathcal{L}}$ and γ.
- the size of the output set $\boldsymbol{S}$ by the algorithm can be represented by parameter γ: $|\boldsymbol{S}| \leq O(n/(\alpha\gamma) \cdot M^{\alpha\gamma})$, where $\alpha = nM/(M-1)$ and $M \geq 2$ is an integer.

Our definition for V-RSP only depends on the parameter γ. The size of the output set by the algorithm for V-RSP is a function of γ. Therefore, we establish relationships between the size of the output set $\boldsymbol{S}$ and the remoteness parameter γ. The algorithm for RSP in [13] is also applied to solve V-RSP (see Algorithm 1). The algorithm for V-RSP outputs the set $\boldsymbol{S}$ of vectors as a linear combinations of the basis vectors with all coefficients in $\{0, 1/M, \ldots, 1-1/M\}$ where $M \geq 2$ by partitioning the n basis vectors into n/k sets of size $k = \lfloor (nM/c(M-1)) \cdot \gamma \rfloor \geq 1$. We show that the deterministic algorithm that on input rank n lattice $\boldsymbol{\mathcal{L}}$ and $\gamma \leq 1$ outputs a set $\boldsymbol{S}$ of size $|\boldsymbol{S}| \leq O(n/k \cdot M^k)$ containing at least one points which is $(1-1/M) \cdot k/n \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ far from $\boldsymbol{\mathcal{L}}$. Moreover, we show that the complexity classes that V-RSP belong to with the change of parameter γ. Using the triangle inequality of norm, the analysis for V-RSP can be adapted to any ℓ_p norm for $1 \leq p \leq \infty$. In the analysis of the algorithm for V-RSP, we use Hölder's Inequality to obtain that the output set containing a point has ℓ_2 distance from a lattice compared with the covering radius in any ℓ_p norm for $1 \leq p \leq \infty$. We also prove that the relationships between the output set containing a point has ℓ_2 distance from a lattice and $\rho^{(p)}(\boldsymbol{\mathcal{L}})$ for $1 \leq p \leq \infty$. For $p = \infty$, we do not rely on Komlós Conjecture which is essential in [13]. We also obtain that the relationships between ℓ_p distance for $1 \leq p \leq \infty$ and $\rho^{(2)}(\boldsymbol{\mathcal{L}})$.

Relation to Haviv's RSP. This paper is inspired by Haviv's, but differs from it in most of details. The definition for RSP in [13] depends on two parameters d, $\gamma \geq 1$ to be minimized, where d is the size of the set constructed and γ is the remoteness parameter. By the analysis the algorithm for RSP, Haviv showed that a deterministic time algorithm for RSP that on full-rank lattice $\boldsymbol{\mathcal{L}}$ outputs a set $\boldsymbol{S}$ of points, at least one of which is $O(\sqrt{k/n}) \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ in any ℓ_p norm for $2 \leq p \leq \infty$. Hence, the distance from the lattice of at least one of the points in $\boldsymbol{S}$ approximates the covering radius to within a factor of $O(\sqrt{k/n})$. Haviv also showed a polynomial time deterministic algorithm outputs a set of points, at least one of which is $\sqrt{\log n/n} \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ far from $\boldsymbol{\mathcal{L}}$ for $2 \leq p \leq \infty$. The proof techniques in [13] involved a theorem on balancing vectors [5] and six standard deviations theorem [19] of Spencer from Banach space theory, and specially depended on Komlós Conjecture for ℓ_∞ norm. All the analysis of Haviv's algorithm for RSP in [13] is hold in any ℓ_p norm for $2 \leq p \leq \infty$.

Our definition for V-RSP only depends on parameter $\gamma \leq 1$, the size of the set is bounded by γ and can not minimize arbitrarily. We prove that the output of the deterministic time algorithm for V-RSP contains a point in $\boldsymbol{S}$ whose distance from lattice $\boldsymbol{\mathcal{L}}$ is at least $O(k/n) \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ in any ℓ_p norm for $1 \leq p \leq \infty$. This implies that the distance of a point in $\boldsymbol{S}$ from the lattice approximates the covering radius to within a factor of $O(k/n)$. Moreover, when we choose $k = \lfloor M/(M-1) \cdot \sqrt{n \cdot \log_M n} \rfloor$, we also obtain that the set S containing a point which is $\sqrt{\log_M n/n} \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$ far from $\boldsymbol{\mathcal{L}}$ for $1 \leq p \leq \infty$ in a deterministic time. The approximation factor is similar to Haviv's $\sqrt{\log n/n}$. We also analyze the complexity of V-RSP. The proof techniques for V-RSP only use some elementary inequalities involving triangle inequality of norm and Hölder's Inequality. And our results for V-RSP are adapted to any ℓ_p norm for $1 \leq p \leq \infty$.

Organization. The rest of the paper is organized as follows. In Sect. 2 we introduce basic notations about lattices and some important inequalities that we need in the paper. In Sect. 3 we propose the variant of Remote Set Problem (V-RSP) and analyze V-RSP.

2 Preliminaries

Let $\mathbb{R}^m$ be a m-dimensional Euclidean space. A norm $\|\cdot\|$ is a positive real-valued function on $\mathbb{R}^m$ that satisfies the triangle inequality, i.e., a function $\|\cdot\| : \mathbb{R}^m \longrightarrow \mathbb{R}$ such that

- $\|\boldsymbol{x}\| \geq 0$ with equality only if $\boldsymbol{x} = \boldsymbol{0}$.
- $\|k\boldsymbol{x}\| = |k|\|\boldsymbol{x}\|$.
- $\|\boldsymbol{x} + \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$.

for all $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^m$ and $k \in \mathbb{R}$. For $1 \leq p < \infty$, the ℓ_p norm of a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_m) \in \mathbb{R}^m$ is defined as $\|\boldsymbol{x}\|_p = (\sum_{i=1}^m |x_i|^p)^{1/p}$ and for $p = \infty$ the ℓ_∞ norm is defined as $\|\boldsymbol{x}\|_\infty = \max\limits_{1 \leq i \leq m} |x_i|$. The ℓ_p distance between two vector $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^m$ is defined as $dist_p(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|_p$. For any vector $\boldsymbol{x} \in \mathbb{R}^m$ and any set $\boldsymbol{S} \subseteq \mathbb{R}^m$, the ℓ_p distance from $\boldsymbol{x}$ to $\boldsymbol{S}$ is $dist_p(\boldsymbol{x}, \boldsymbol{S}) = \min\limits_{\boldsymbol{y} \in \boldsymbol{S}} dist_p(\boldsymbol{x}, \boldsymbol{y})$.

A lattice $\boldsymbol{\mathcal{L}}$ is the set of all linear combinations that generated by n linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ in $\mathbb{R}^m (m \geq n)$, that is

$$\boldsymbol{\mathcal{L}} = \{\sum_{i=1}^{n} x_i \boldsymbol{b}_i | x_i \in \mathbb{Z}, 1 \leq i \leq n\}.$$

The integer n is the rank of the lattice, m is the dimension of the lattice. The sequence of linear independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$ is called a basis of the lattice. We represent $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ by the matrix $\boldsymbol{B}$ of m rows and n columns, that is, $\boldsymbol{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n] \in \mathbb{R}^{m \times n}$. The lattice $\boldsymbol{\mathcal{L}}$ generated by a basis $\boldsymbol{B}$ is denoted by $\boldsymbol{\mathcal{L}} = \boldsymbol{\mathcal{L}}(\boldsymbol{B}) = \{\boldsymbol{B}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\}$.

In the following, we consider the covering radius which is an important parameter associated with lattices.

Definition 1 (Covering Radius). *The covering radius of $\boldsymbol{\mathcal{L}}$, denoted $\rho(\boldsymbol{\mathcal{L}})$, is defined as the smallest radius ρ such that the (closed) spheres of radius ρ centered at all lattice points cover the entire space, i.e., any point in span($\boldsymbol{\mathcal{L}}$) is within distance ρ from the lattice.*

Formally, the covering radius $\rho^{(p)}(\boldsymbol{\mathcal{L}})$ is defined as the maximum distance $dist_p(\boldsymbol{x}, \boldsymbol{\mathcal{L}})$:

$$\rho^{(p)}(\boldsymbol{\mathcal{L}}) = \max_{\boldsymbol{x} \in span(\boldsymbol{\mathcal{L}})} dist_p(\boldsymbol{x}, \boldsymbol{\mathcal{L}}),$$

where $\boldsymbol{x}$ ranges over the linear span of $\mathcal{L}$.

There exists a set of all the vector as a linear combinations of the basis vectors with all coefficients in $\{0, 1/M, \ldots, 1 - 1/M\}$. The following lemma shows that at least one of the points in the set is quite far from the lattice.

Lemma 1 [10]**.** *For every $1 \leq p \leq \infty$, any basis $\boldsymbol{B}$ and an integer $M > 0$, there exists a point*

$$\boldsymbol{v} = a_1\boldsymbol{b}_1 + \cdots + a_n\boldsymbol{b}_n$$

such that $a_i \in \{0, 1/M, \ldots, 1 - 1/M\}$ for all i, and $dist_p(\boldsymbol{v}, \boldsymbol{\mathcal{L}}) \geq (1 - 1/M) \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$.

The definition of the variant of Remote Set Problem (V-RSP) for any $1 \leq p \leq \infty$ and $\gamma \leq 1$ is in the following.

Definition 2 ($V\text{-}RSP_{\gamma}^{(p)}$). *For an integer $M \geq 2$, given a lattice basis $\boldsymbol{B} \in \mathbb{Q}^{m \times n}$ and $\gamma \leq 1$, the variant of Remote Set Problem is to find a set $\boldsymbol{S} \subseteq span(\boldsymbol{\mathcal{L}})$ of size $|\boldsymbol{S}| \leq O(n/(\alpha\gamma) \cdot M^{\alpha\gamma})$ such that S contains a point $\boldsymbol{v}$ satisfying*

$$dist_p(\boldsymbol{v}, \boldsymbol{\mathcal{L}}) \geq \gamma \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}})$$

where $\alpha = nM/(M-1)$.

The following inequalities are essential in this paper.

Lemma 2 (Equivalent Norms [9]**).** *Let $\|\cdot\|_\alpha$ and $\|\cdot\|_\beta$ be two different norms on the same vector space V. There exists positive constants t, T such that*

$$t\|\boldsymbol{x}\|_\alpha \leq \|\boldsymbol{x}\|_\beta \leq T\|\boldsymbol{x}\|_\alpha$$

for any vector $\boldsymbol{x} \in V$.

Theorem 1 (Hölder's Inequality [9]**).** *Fix an arbitrary norm $\|\cdot\|$ on $\mathbb{R}^m$, for any vector $\boldsymbol{x} \in \mathbb{R}^m$, we have the following inequalities:*

- *for any $1 \leq p \leq 2$, $\|\boldsymbol{x}\|_2 \leq \|\boldsymbol{x}\|_p \leq m^{1/p-1/2}\|\boldsymbol{x}\|_2$,*
- *for any $2 < p < \infty$, $m^{1/p-1/2}\|\boldsymbol{x}\|_2 \leq \|\boldsymbol{x}\|_p \leq \|\boldsymbol{x}\|_2$,*
- *for $p = \infty$, $\frac{1}{\sqrt{m}}\|\boldsymbol{x}\|_2 \leq \|\boldsymbol{x}\|_\infty \leq \|\boldsymbol{x}\|_2$.*

3 The Variant of Remote Set Problem

3.1 Algorithm for the Variant of Remote Set Problem

In this section, based on Definition 2, we use triangle inequality to analyze the algorithm for V-RSP which applies to any ℓ_p norm for $1 \leq p \leq \infty$.

Theorem 2. *For an integer $M \geq 2$, for every $1 \leq p \leq \infty$ and every $k = k(n,\gamma) = \lfloor \frac{nM}{c(M-1)}\gamma \rfloor \geq 1$, there exists a deterministic $M^k \cdot b^{O(1)}$ time algorithm for V-RSP$_\gamma^{(p)}$ that on input a lattice basis $\boldsymbol{B} \in \mathbb{Q}^{m\times n}$ and $\gamma \leq 1$, outputs a set $\boldsymbol{S}$ of size $|\boldsymbol{S}| = O(n/k \cdot M^k) = O(n/(\alpha\gamma) \cdot M^{\alpha\gamma})$ containing a point which is quite far from a lattice, where $\alpha = nM/(M-1)$, n denotes lattice rank, m denotes lattice dimension, b is the input size, c is a constant.*

Proof. Our proof is similar to [13], but our technique is different since we only use the triangle inequality of norm. We will give full proof for completeness here.

Assume that $k = k(n,\gamma)$ divides n. First, we partition the lattice basis $\boldsymbol{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ into n/k sets of size k each, i.e., $\boldsymbol{B} = (\boldsymbol{B}_1, \boldsymbol{B}_2, \ldots, \boldsymbol{B}_{n/k})$. Then the algorithm outputs a set $\boldsymbol{S}$ containing $n/k \cdot M^k$ vectors in span$(\boldsymbol{B})$ that are linear combinations of vectors in $\boldsymbol{B}_i$ with coefficients in $\{0, 1/M, \ldots, 1-1/M\}$. These vectors must be in some $\boldsymbol{S}_i, i = 1, 2, \ldots, n/k$.

For every $1 \leq i \leq n/k$, $j = 1, 2, \ldots, k$,

$$\boldsymbol{S}_i = \{v | v = a_1\boldsymbol{b}_{(i-1)k+1} + a_2\boldsymbol{b}_{(i-1)k+2} + \cdots + a_k\boldsymbol{b}_{ik}\}$$

where $a_j \in \{0, 1/M, \ldots, 1-1/M\}$. The algorithm outputs $\boldsymbol{S} = \bigcup_{i=1}^{n/k} \boldsymbol{S}_i$. Hence, we have $|\boldsymbol{S}| \leq n/k \cdot M^k$ and obtain $\boldsymbol{S}$ in time $M^k \cdot b^{O(1)}$, where b is the input size.

For $1 \leq p \leq \infty$, we claim that there exists a vector $\boldsymbol{w}$ in $\boldsymbol{S}$ such that ℓ_p distance from $\boldsymbol{\mathcal{L}}(\boldsymbol{B})$ is at least $(1-1/M)\cdot k/n \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$, i.e., $dist_p(w, \boldsymbol{\mathcal{L}}(\boldsymbol{B})) \geq (1-1/M) \cdot k/n \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$. Assume for contradiction that for every vector $\boldsymbol{v}$ in $\boldsymbol{S}$ there exists a lattice vector $\boldsymbol{y}$ such that

$$dist_p(\boldsymbol{v}, \boldsymbol{y}) < (1-1/M) \cdot k/n \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B})).$$

By Lemma 1, there exists a point $\boldsymbol{v} = a_1\boldsymbol{b}_1 + a_2\boldsymbol{b}_2 + \cdots + a_n\boldsymbol{b}_n$ such that $a_i \in \{0, 1/M, \ldots, 1-1/M\}$ for all i and $dist_p(\boldsymbol{v}, \boldsymbol{\mathcal{L}}(\boldsymbol{B})) \geq (1-1/M)\cdot\rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$.

Let

$$\boldsymbol{v} = \boldsymbol{v}_1 + \boldsymbol{v}_2 + \cdots + \boldsymbol{v}_{n/k}$$

where $\boldsymbol{v}_i = a_{(i-1)k+1}\boldsymbol{b}_{(i-1)k+1} + a_{(i-1)k+2}\boldsymbol{b}_{(i-1)k+2} + \cdots + a_{ik}\boldsymbol{b}_{ik}$, $a_j \in \{0, 1/M, \ldots, 1-1/M\}$ for $j = (i-1)k+1, \ldots, ik$, $1 \leq i \leq n/k$.

Clearly, $\boldsymbol{v}_i \in \boldsymbol{S}_i \subseteq \boldsymbol{S}$, by assumption that there exists a lattice vector $\boldsymbol{y}_i \in \boldsymbol{\mathcal{L}}(\boldsymbol{B})$ such that

$$dist_p(\boldsymbol{v}_i, \boldsymbol{y}_i) = \|\boldsymbol{v}_i - \boldsymbol{y}_i\|_p < (1 - \frac{1}{M}) \cdot \frac{k}{n} \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B})).$$

Algorithm 1. The Variant of Remote Set Problem ([13]).

Input:

A lattice basis $\boldsymbol{B} = (\boldsymbol{B}_1, \boldsymbol{B}_2, \ldots, \boldsymbol{B}_{n/k}) \in \mathbb{Q}^{m \times n}$, γ.

Output:

A set $\boldsymbol{S} \subseteq span(\boldsymbol{B})$ of $n/k \cdot M^k$ vectors at least one of which is $(1 - 1/M) \cdot n/k \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$ far from $\boldsymbol{\mathcal{L}}(\boldsymbol{B})$.

For every $1 \leq i \leq n/k$

1.Define $\boldsymbol{B}_i = [\boldsymbol{b}_{(i-1)k+1}, \ldots, \boldsymbol{b}_{ik}]$.

2.Construct the set

$\boldsymbol{S}_i = \{v | v = a_1\boldsymbol{b}_{(i-1)k+1} + a_2\boldsymbol{b}_{(i-1)k+2} + \cdots + a_k\boldsymbol{b}_{ik}\}$,

where $a_j \in \{0, 1/M, \ldots, 1 - 1/M\}$.

Return $\boldsymbol{S} = \bigcup_{i=1}^{n/k} S_i$.

For every $1 \leq i \leq n/k$, let $\boldsymbol{\beta}_i = \boldsymbol{v}_i - \boldsymbol{y}_i$. Using the triangle inequality, we have

$$\begin{aligned} \|\sum_{i=1}^{n/k} \boldsymbol{\beta}_i\|_p &\leq \|\boldsymbol{\beta}_1\|_p + \|\boldsymbol{\beta}_2\|_p + \cdots + \|\boldsymbol{\beta}_{n/k}\|_p \\ &< (1 - \frac{1}{M}) \cdot \frac{n}{k} \cdot \frac{k}{n} \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B})) \\ &= (1 - \frac{1}{M}) \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B})). \end{aligned}$$

Since

$$\boldsymbol{v} - \sum_{i=1}^{n/k} \boldsymbol{\beta}_i = \sum_{i=1}^{n/k} \boldsymbol{v}_i - \sum_{i=1}^{n/k} \boldsymbol{\beta}_i = \sum_{i=1}^{n/k} \boldsymbol{y}_i \in \boldsymbol{\mathcal{L}}(\boldsymbol{B}),$$

we have

$$\begin{aligned} dist_p(\boldsymbol{v}, \boldsymbol{\mathcal{L}}(\boldsymbol{B})) &= dist_p(\sum_{i=1}^{n/k} \boldsymbol{\beta}_i, \boldsymbol{\mathcal{L}}(\boldsymbol{B})) \\ &\leq \|\sum_{i=1}^{n/k} \boldsymbol{\beta}_i\|_p \\ &< (1 - \frac{1}{M}) \cdot \rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B})). \end{aligned}$$

This contradicts the choice of $\boldsymbol{v}$. So, there exists a vector in $\boldsymbol{S}$ whose ℓ_p distance from $\boldsymbol{\mathcal{L}}(\boldsymbol{B})$ is quite far.

Using the triangle inequality, the algorithm for V-RSP is also holding in any ℓ_p norm for $1 \leq p \leq \infty$ and solves the case of $1 \leq p < 2$. When $M = 2$, we can obtain a similar result to Haviv (see [13], Theorem 3.1), though our approximation factor is a little weaker. However, our techniques are simpler.

By choosing $k = \lfloor cM/(M-1) \cdot \sqrt{n \log_M n} \rfloor$, where c is a constant and n is the lattice rank, we will derive that the output of our algorithm contains a point

whose distance from lattice $\boldsymbol{\mathcal{L}}$ is at least $\sqrt{\log_M n/n}\cdot\rho^{(p)}(\boldsymbol{\mathcal{L}})$. This approximation factor is similar to Haviv's. We will describe in the following.

Corollary 1. *For an integer $M \geq 2$, for every $1 \leq p \leq \infty$ and $k = \lfloor cM/(M-1)\cdot\sqrt{n\log_M n}\rfloor$, there exists a deterministic time algorithm for V-RSP$_\gamma^{(p)}$ that on input a lattice $\boldsymbol{B} \in \mathbb{Q}^{m\times n}$ and $\gamma \leq 1$, outputs a set containing a point which is $\sqrt{\log_M n/n}\cdot\rho^{(p)}(\boldsymbol{\mathcal{L}})$ far from lattice $\boldsymbol{\mathcal{L}}$, where n denotes lattice rank and c is a constant.*

3.2 The Complexity Classes for V-RSP

We will analyze the complexity classes for V-RSP$_\gamma^{(p)}$ with the change of parameter γ, as stated in the following.

1. For every $1 \leq p \leq \infty$ and $0 \leq \epsilon \leq 1$, for $\frac{1}{n}(1-\frac{1}{M}) \leq \gamma \leq \frac{\log_M^\epsilon n}{n}(1-\frac{1}{M})$, there exists a deterministic polynomial time algorithm for V-RSP$_\gamma^{(p)}$, and V-RSP$_\gamma^{(p)}$ lies in Class P.
2. For every $1 \leq p \leq \infty$ and $\epsilon > 1$, for $\frac{\log_M n}{n}(1-\frac{1}{M}) \leq \gamma \leq \frac{\log_M^\epsilon n}{n}(1-\frac{1}{M})$, there exists a deterministic (single) exponential time algorithm for V-RSP$_\gamma^{(p)}$.

3.3 An Additional Property of V-RSP

By the Theorem 2, we show that the algorithm for V-RSP can find a set of points containing a point which is far from the lattice. We use the Hölder's Inequality in Theorem 1 to study the relationships between the ℓ_2 distance from a point of the output set to a lattice $\boldsymbol{\mathcal{L}}$ and the covering radius ($\rho^{(p)}(\boldsymbol{\mathcal{L}})$) of the lattice $\boldsymbol{\mathcal{L}}$ for every $1 \leq p \leq \infty$. The case of $1 \leq p < 2$ is not mentioned in [13]. Specially, when $p = \infty$, we do not depend on Komlós Conjecture. Similar to [13], the following theorems are based on algorithm presented in the proof of Theorem 2.

Theorem 3. *For an integer $M \geq 2$, for every $1 \leq p \leq 2$ and every $k = k(n,\gamma) = \lfloor\frac{nM}{c(M-1)}\gamma\rfloor \geq 1$, there exists a deterministic $M^k\cdot b^{O(1)}$ time algorithm for V-RSP$_\gamma^{(p)}$ that on input a lattice basis $\boldsymbol{B} \in \mathbb{R}^m$ and $\gamma \leq 1$ outputs a set $\boldsymbol{S}$ of size $|\boldsymbol{S}| = O(n/k\cdot M^k) = O(n/(\alpha\gamma)\cdot M^{\alpha\gamma})$ containing a point whose ℓ_2 distance from $\boldsymbol{\mathcal{L}}$ is at least $1/m^{1/p-1/2}\cdot(1-1/M)\cdot k/n\cdot\rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$, where $\alpha = nM/(M-1)$, m denotes lattice dimension, b is the input size, c is a constant. For a special case of full-rank lattice($m = n$), one of the points whose ℓ_2 distance is at least $k/n^{1/p+1/2}\cdot(1-1/M)\cdot\rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$.*

Theorem 4. *For an integer $M \geq 2$, for every $2 < p \leq \infty$ and every $k = k(n,\gamma) = \lfloor\frac{nM}{c(M-1)}\gamma\rfloor \geq 1$, there exists a deterministic $M^k\cdot b^{O(1)}$ time algorithm for V-RSP$_\gamma^{(p)}$ that on input a lattice $\boldsymbol{B} \in \mathbb{R}^m$ and $\gamma \leq 1$, outputs a set $\boldsymbol{S}$ of size $|\boldsymbol{S}| = O(n/k\cdot M^k) = O(n/(\alpha\gamma)\cdot M^{\alpha\gamma})$ containing a point whose ℓ_2 distance from $\boldsymbol{\mathcal{L}}$ is at least $(1-1/M)\cdot k/n\cdot\rho^{(p)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$, where $\alpha = nM/(M-1)$, m denotes lattice dimension, b is the input size, c is a constant.*

In the following, we study the relationships between the $\ell_p (1 \leq p \leq \infty)$ distance from a point of the output set to a lattice $\boldsymbol{\mathcal{L}}$ and the covering radius $(\rho^{(2)}(\boldsymbol{\mathcal{L}}))$ of the lattice $\boldsymbol{\mathcal{L}}$.

Corollary 2. *For an integer $M \geq 2$, for every $1 \leq p \leq 2$ and every $k = k(n,\gamma) = \lfloor \frac{nM}{c(M-1)}\gamma \rfloor \geq 1$, there exists a deterministic $M^k \cdot b^{O(1)}$ time algorithm for V-RSP$_\gamma^{(p)}$ that on input a lattice $\boldsymbol{B} \in \mathbb{R}^m$ and $\gamma \leq 1$ outputs a set $\boldsymbol{S}$ of size $|\boldsymbol{S}| = O(n/k \cdot M^k)$ containing a point whose ℓ_p distance from $\boldsymbol{\mathcal{L}}$ is at least $(1 - 1/M) \cdot k/n \cdot \rho^{(2)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$. For every $2 < p < \infty$, one of points whose ℓ_p distance is at least $1/m^{1/p-1/2} \cdot (1 - 1/M) \cdot k/n \cdot \rho^{(2)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$. For a the full-rank lattice $(m = n)$, one of the points whose ℓ_p distance is at least $k/n^{1/p+1/2} \cdot (1 - 1/M) \cdot \rho^{(2)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$, where m denotes lattice dimension, b is the input size, c is a constant.*

Corollary 3. *For an integer $M \geq 2$, for every $p = \infty$ and every $k = k(n,\gamma) = \lfloor \frac{nM}{c(M-1)}\gamma \rfloor \geq 1$, there exists a deterministic $M^k \cdot b^{O(1)}$ time algorithm for V-RSP$_\gamma^{(p)}$ that on input a lattice $\boldsymbol{B} \in \mathbb{R}^m$ and $\gamma \leq 1$ outputs a set $\boldsymbol{S}$ of size $|\boldsymbol{S}| = O(n/k \cdot M^k)$ containing a point whose ℓ_p distance from $\boldsymbol{\mathcal{L}}$ is at least $1/\sqrt{m} \cdot (1 - 1/M) \cdot k/n \cdot \rho^{(2)}(\boldsymbol{\mathcal{L}}(\boldsymbol{B}))$, where m denotes lattice dimension, b is the input size, c is a constant.*

4 Conclusion

In our paper, we propose the variant of Remote Set Problem (V-RSP) which only relies on the parameter $\gamma \leq 1$. From the algorithm for RSP, we knew that the distance from the lattice of at least one of the point in the set $\boldsymbol{S}$ approximates the covering radius to within a factor of $O(\sqrt{k/n})$ in ℓ_p norm for $2 \leq p \leq \infty$. However, using some elementary tools, we obtain that the approximation is $O(k/n)$ in the algorithm for V-RSP in ℓ_p norm for $1 \leq p \leq \infty$. This introduces a $O(\sqrt{k/n})$ loss in the approximation factors. We also can get the same approximation factors at the cost of more time in the algorithm for V-RSP. Hence, there is an interesting problem to reduce the gap between RSP and V-RSP.

Acknowledgements. This work was supported by National Natural Science Foundation of China (Grant No. 61272039).

References

1. Aharonov, D., Regev, O.: Lattice problems in NP intersect coNP. J. ACM **52**(5), 749–765 (2005). Preliminary version in FOCS 2004
2. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: 28th Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996), pp. 99–108. ACM, New York (1996)

3. Ajtai, M.: The shortest vector problem in ℓ_2 is NP-hard for randomized reductions (extended abstract). In: 30th ACM Symposium on the Theory of Computing, pp. 10-19 (1998)
4. Ajtai, M., Kumar, R., Sivakumar, D.: A Sieve algorithm for the shortest lattice vector problem. In: 33th ACM Symposium on Theory of Computing, pp. 601–610 (2001)
5. Banaszczyk, W.: Balancing vectors and Gaussian measures of n-dimensional convex bodies. Random Struct. Algorithm **12**(4), 351–360 (1998)
6. Dinur, I., Kindler, G., Raz, R., Safra, S.: Approximating CVP to within almost-polynomial factors is NP-hard. Combinatorica **23**(2), 205–243 (2003)
7. Gauss, C.F.: Disquisitiones Arithmeticae, Gerh. Fleischer Iun, Lipsia (1801)
8. Goldreich, O., Goldwasser, S.: On the limits of nonapproximability of lattice problems. J. Comput. Syst. Sci. **60**(3), 540–563 (2000)
9. Griffel, D.H.: Applied Functional Analysis. Horwood Limited, Chichester (2002)
10. Guruswami, V., Micciancio, D., Regev, O.: The complexity of the covering radius problem on lattices and codes. Comput. Complex. **14**(2), 90–121 (2005). Preliminary version in CCC 2004
11. Haviv, I., Regev, O.: Tensor-based hardness of the shortest vector problem to within almost polynomial factors. Theory Comput. **8**, 513–531 (2012)
12. Haviv, I., Regev, O.: Hardness of the covering radius problem on lattices. Chicago J. Theoret. Comput. Sci. **04**, 1–12 (2012)
13. Haviv, I.: The remote set problem on lattice. Comput. Complex. **24**(1), 103–131 (2015)
14. Khot, S.: Hardness of approximating the shortest vector problem in lattices. J. ACM (JACM) **52**(5), 789–808 (2005)
15. Lenstra, A., Lenstra, H., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**, 515–534 (1982)
16. Micciancio, D.: Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. SIAM J. Comput **34**, 118–169 (2004)
17. Micciancio, D., Voulgaris, P.: A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computation. Soc. Ind. Appl. Math., SIAM J. Comput. **42**(3), 1364–1391 (2013)
18. Peikert, C.: Limits on the hardness of lattice problems in ℓ_p norms. Comput. Complex. **17**(2), 300–335 (2008). Preliminary version in CCC 2007
19. Spencer, J.: Six standard deviations suffice. Trans. Am. Math. Soc. **289**(2), 679–706 (1985)
20. Van Emde Boas, P.: Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report 8104, Department of Mathematics, University of Amsterdam, Netherlands (1981)